REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1, 2, 3, 9, 15, and 18 are amended. Claims 25 and 34 are canceled without prejudice. New claims 35 and 36 are added. Claims 1-24, 26, 31-33, and 35-36 are pending in this application.

Interview Summary

Applicant thanks Examiner Benjamin Lanier and Examiner Gilberto Barron for the telephone interview of March 2, 2004 between Examiners Lanier and Barron and Applicant's undersigned representative. In the March 2, 2004 interview, independent claims 1, 2, 9, 15, 18, and 31 were discussed, although no agreement as to the allowability of any of the claims was reached. The Yoshida (U.S. Patent No. 6,075,862) and Easter (U.S. Patent No. 5,563,950) references were discussed, as well as the new matter objection and 35 U.S.C. §112, first paragraph rejection. Applicant's undersigned representative argued where support for the rejected claim language could be found in the specification, and argued deficiencies in the combination of Yoshida and Easter. The Examiners argued that they felt support for some of the rejected claim language could not be found in the specification, and argued that the combination of Yoshida and Easter was sufficient for the rejection. Possible claim amendments to positively recite elements of the installation module and overcome the new matter objection and 35 U.S.C. §112, first paragraph rejection were discussed. Portions of the specification supporting the claim amendments subject to the 35 U.S.C. §112, first paragraph rejection were also discussed.

35 U.S.C. § 132

In the September 29, 2003 Office Action, it was asserted that the amendment filed August 26, 2003 introduced new matter into the disclosure. Specifically, the September 29, 2003 Office Action asserted that the added material which was not supported by the original disclosure was: "The trigger file consists of only content other than a decryption key, determining which of a first and second version of software to install wherein a first version of the multiple has greater than a threshold strength encryption, and wherein a second version of the multiple versions has not greater than the threshold strength encryption, and the threshold strength encryption comprising 56-bit encryption."

These objections to the claims are discussed below in under the section heading 35 U.S.C. §112.

35 U.S.C. § 112

Claims 1, 9, 15, and 31-34 stand rejected under 35 U.S.C. §112, first paragraph due to the asserted new matter. Claim 34 has been canceled without prejudice, thereby rendering the rejection of claim 34 moot.

With regard to claims 1, 9, and 15, Applicant respectfully disagrees with the rejection and submits that claims 1, 9, and 15 do comply with 35 U.S.C. §112, first paragraph. However, in order to advance prosecution and expedite allowance of the present application, claims 1, 9, and 15 have been amended to clarify the language of claims 1, 9, and 15.

With regard to claims 31-34, the Examiner is directed to the specification at, for example, p. 11, lines 7-19, which recites:

> The setup program invokes the installation module, which in turn decrypts and installs the restricted software modules only when one or more trigger files are present on computer 20. If none of the trigger files are present on computer 20, then, in one embodiment, the setup program installs a non-restricted version of the software module. In this manner, the installation modules securely install the restricted software modules only when computer 20 is authorized. For example, in one embodiment the restricted software modules are domestic strength cryptographic software modules. In this embodiment the installation modules securely install domestic strength cryptographic software only when computer 20 is authorized to use such software.

Furthermore, domestic and international versions of software, as well as regulations prohibiting exporting software having more than 56-bit encryption are discussed in the specification at page 1, lines 9-17.

Thus, for at least these reasons, Applicant respectfully submits that claims 1, 9, 15, and 31-33 comply with 35 U.S.C. §112, first paragraph.

Applicant respectfully requests that the §112 rejections be withdrawn.

35 U.S.C. § 102

Claims 1, 8-11, 14-16, 19, 20, 22-24, and 31-34 stand rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Patent No. 6,075,862 to Yoshida et al. (hereinafter "Yoshida"). Claim 34 has been canceled without prejudice, thereby rendering the rejection of claim 34 moot. Applicant respectfully submits that claims 1, 8-11, 14-16, 19, 20, 22-24, and 31-33 are not anticipated by Yoshida.

Yoshida is directed to a decryption key management scheme for a software distribution system (see, col. 1, lines 1-9). The software ID and decryption key for software are stored into a decryption key memory unit on a computer's hard disk drive (see, col. 6, lines 1-14, and Fig. 1). Yoshida further discloses that when re-installing the software that was already installed once, it is possible to decrypt the encrypted software content immediately by utilizing the decryption key stored in the decryption key memory unit (see, col. 7, lines 13-20). When the software is installed for the first time, the decryption key will be automatically acquired from the software vendor (see, col. 7, lines 13-20). The decryption key is acquired from the software vendor through a communication network in exchange for payment of a software usage charge (see, col. 6, lines 41-53).

Amended claim 1 recites:

> 1. An installation module comprising:
> an encrypted software module;
> a decryption key to decrypt the encrypted software module; and
> an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system, wherein each of the trigger files indicates authorization to install the encrypted software module.

Applicant respectfully submits that an installation module having an encrypted software module, a decryption key, and an executive as recited in claim 1 is not disclosed by Yoshida.

As discussed above, Yoshida discloses obtaining the decryption key from the hard disk of the computer on which the software is to be installed or from the software vendor through a communication network in exchange for payment of a software usage charge. Neither of these methods of obtaining the decryption key

in Yoshida discloses an installation module that includes an encrypted software module as well as the decryption key to decrypt the encrypted software module.

Thus, for at least these reasons, Applicant respectfully submits that amended claim 1 is allowable over Yoshida.

Given that claim 8 depends from amended claim 1, Applicant respectfully submits that claim 8 is likewise allowable over Yoshida for at least the reasons discussed above with respect to amended claim 1.

With respect to amended claim 9, Applicant respectfully submits that, similar to the discussion above regarding amended claim 8, Yoshida does not disclose a software system comprising an installation module comprising an encrypted software module, a decryption key, and an executive as recited in amended claim 9. For at least these reasons, Applicant respectfully submits that amended claim 9 is allowable over Yoshida.

Given that claims 10, 11, and 14 depend from amended claim 9, Applicant respectfully submits that claims 10, 11, and 14 are likewise allowable over Yoshida for at least the reasons discussed above with respect to amended claim 9.

With respect to amended claim 15, Applicant respectfully submits that, similar to the discussion above regarding amended claim 1, Yoshida does not disclose decrypting an encrypted software module using a decryption key included with the encrypted software module when at least one of a set of trigger files is stored on a computing system as recited in amended claim 15. For at least these reasons, Applicant respectfully submits that amended claim 15 is allowable over Yoshida.

Given that claims 16, 19, 20, 22, and 23 depend from amended claim 15, Applicant respectfully submits that claims 16, 19, 20, 22, and 23 are likewise allowable over Yoshida for at least the reasons discussed above with respect to amended claim 15.

With respect to claim 24, claim 24 recites:

> 24. One or more computer-readable media having stored thereon a plurality of instructions that, when executed by one or more processors, cause the one or more processors to:
>
> decrypt an encrypted software module when a trigger file is stored on a computing system, wherein the trigger file comprises a prior version of the encrypted software module; and
>
> load the decrypted software module onto the computing system.

Applicant respectfully submits that Yoshida does not disclose or suggest decryption of an encrypted software module when a trigger file is stored on a computing system, wherein the trigger file comprises a prior version of the encrypted software module as recited in claim 24.

As discussed above, Yoshida discloses that the software ID and decryption key for software are stored into a decryption key memory unit on a computer's hard disk drive, and when re-installing the software that was already installed once, it is possible to decrypt the encrypted software content immediately by utilizing the decryption key stored in the decryption key memory unit. When the software is installed for the first time, the decryption key will be automatically acquired from the software vendor through a communication network in exchange for payment of a software usage charge.

In the September 29 Office Action, it appears that the decryption key of Yoshida is being relied on as disclosing the trigger file of claim 24 (see,

September 29 Office Action at ¶ 7, p. 4). However, Applicant respectfully submits that the decryption key of Yoshida does not satisfy the language of claim 24, particularly the "wherein the trigger file comprises a prior version of the encrypted software module" as recited in claim 24. If the decryption key of Yoshida were to be the trigger file of claim 24, then the decryption key would need to be "a prior version of the encrypted software module". However, the decryption key in Yoshida is simply that – a decryption key. Nowhere does Yoshida make any mention of the decryption key of Yoshida being a previous version of an encrypted software module. Furthermore, Applicant respectfully submits that decryption keys are not part of the software being installed in Yoshida. As discussed above, when installing software, the decryption key may already be on the computer's hard disk drive, or may be obtained from the software vendor in exchange for payment of a software usage charge – nothing in either of these methods of obtaining the decryption key discloses the decryption key being part of the software being installed in Yoshida. Therefore, the decryption key of Yoshida could not be a prior version of an encrypted software module.

Thus, for at least these reasons, Applicant respectfully submits that claim 24 is allowable over Yoshida.

With respect to claim 26, Applicant notes that there is no basis for rejection of claim 26 indicated in the September 29 Office Action. Accordingly, Applicant respectfully submits that claim 26 is allowable over the cited references.

With respect to claims 31-34, Applicant notes that although the September 29 Office Action indicates that claims 31-34 are rejected under 35 U.S.C. 102(e)

as being anticipated by Yoshida, there is no mention in the September 29 Office Action of where in Yoshida the elements of claims 31-34 are asserted as being disclosed. Applicant respectfully submits that nowhere does Yoshida disclose a method comprising the checking and determining of claim 31. Thus, for at least these reasons, Applicant respectfully submits that claim 31 is allowable over Yoshida.

Given that claims 32-33 depend from claim 31, Applicant respectfully submits that claims 32-33 are likewise allowable over Yoshida for at least the reasons discussed above with respect to claim 31.

Applicant respectfully requests that the §102 rejections be withdrawn.

35 U.S.C. § 103

Claims 4, 6, 12, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yoshida in view of U.S. Patent No. 6,058,478 to Davis (hereinafter "Davis"). Applicant respectfully submits that claims 4, 6, 12, and 21 are not obvious over Yoshida in view of Davis.

With respect to claim 4, claim 4 depends indirectly from claim 2, and Applicant respectfully submits that Davis is not cited as curing, and does not cure, the deficiencies of Yoshida as discussed with respect to claim 2 discussed below. For at least these reasons, Applicant respectfully submits that claim 4 is allowable over Yoshida in view of Davis.

With respect to claim 6, claim 6 depends from claim 1, and Applicant respectfully submits that Davis is not cited as curing, and does not cure, the deficiencies of Yoshida as discussed above with respect to claim 1. For at least

these reasons, Applicant respectfully submits that claim 6 is allowable over Yoshida in view of Davis.

With respect to claim 12, claim 12 depends from claim 9, and Applicant respectfully submits that Davis is not cited as curing, and does not cure, the deficiencies of Yoshida as discussed above with respect to claim 9. For at least these reasons, Applicant respectfully submits that claim 12 is allowable over Yoshida in view of Davis.

With respect to claim 21, claim 21 depends from claim 15, and Applicant respectfully submits that Davis is not cited as curing, and does not cure, the deficiencies of Yoshida as discussed above with respect to claim 15. For at least these reasons, Applicant respectfully submits that claim 21 is allowable over Yoshida in view of Davis.

Claims 7 and 13 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yoshida in view of Davis and further in view of U.S. Patent No. 5,825,890 to Elgamal et al. (hereinafter "Elgamal"). Applicant respectfully submits that claims 7 and 13 are not obvious over Yoshida in view of Davis and Elgamal.

With respect to claim 7, claim 7 depends from claim 6, and Applicant respectfully submits that Elgamal is not cited as curing, and does not cure, the deficiencies of Yoshida and Davis as discussed above with respect to claim 6. For at least these reasons, Applicant respectfully submits that claim 7 is allowable over Yoshida in view of Davis and Elgamal.

With respect to claim 13, claim 13 depends from claim 12, and Applicant respectfully submits that Elgamal is not cited as curing, and does not cure, the

deficiencies of Yoshida and Davis as discussed above with respect to claim 12. For at least these reasons, Applicant respectfully submits that claim 13 is allowable over Yoshida in view of Davis and Elgamal.

Claims 2, 3, and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yoshida in view of U.S. Patent No. 5,563,950 to Easter et al. (hereinafter "Easter"). Applicant respectfully submits that claims 2, 3, and 18 are not obvious over Yoshida in view of Easter.

Yoshida, as discussed above, discloses that the software ID and decryption key for software are stored into a decryption key memory unit on a computer's hard disk drive, and when re-installing the software that was already installed once, it is possible to decrypt the encrypted software content immediately by utilizing the decryption key stored in the decryption key memory unit. When the software is installed for the first time, the decryption key will be automatically acquired from the software vendor through a communication network in exchange for payment of a software usage charge.

Easter, on the other hand, discloses system and methods for encrypting data using public key cryptography (see, col. 1, lines 1-13). Easter discloses that each user has both an individual public key and an individual private key (see, col. 1, lines 53-55). The public key is obtainable from a common database of every user and their respective public key, and the private keys are conventionally entered in the local system by the user through manual entry or insertion of a removable data card with the private key stored thereon (see, col. 1, lines 55-61).

In contrast, amended claim 2 recites:

> 2. An installation module comprising:
> an encrypted software module;

a key;

an executive for decrypting the encrypted software module with the key when at least one of a set of trigger files is stored on a computing system; and

a database for identifying the trigger files.

Applicant respectfully submits that the combination of Yoshida and Easter does not disclose or suggest an installation module as claimed in amended claim 2.

As discussed above, Yoshida discloses obtaining the decryption key from the hard disk of the computer on which the software is to be installed or from the software vendor through a communication network in exchange for payment of a software usage charge. Neither of these methods of obtaining the decryption key in Yoshida discloses or suggests an installation module that includes an encrypted software module as well as a key, used by an executive of the installation module for decrypting an encrypted software module of the installation module as recited in amended claim 2.

With regard to Easter, merely disclosing that a public key is obtainable from a common database of every user and their respective public key does not disclose or suggest an installation module including a key, used by an executive of the installation module for decrypting an encrypted software module of the installation module as recited in amended claim 2.

Thus, for at least these reasons, Applicant respectfully submits that amended claim 2 is allowable over Yoshida in view of Easter.

Given that claim 3 depends from amended claim 2, Applicant respectfully submits that claim 3 is likewise allowable over Yoshida in view of Easter for at least the reasons discussed above with respect to amended claim 2.

With respect to amended claim 18, Applicant respectfully submits that, similar to the discussion of amended claim 2, Yoshida in view of Easter does not

disclose or suggest decrypting an encrypted software module when at least one of a set of trigger files is stored on a computing system, wherein the decrypting includes retrieving a cryptographic key from a database of an installation module that includes the encrypted software module and using the retrieved key to decrypt the encrypted software module as recited in amended claim 18.

Thus, for at least these reasons, Applicant respectfully submits that amended claim 18 is allowable over Yoshida in view of Easter.

Claims 5 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Yoshida in view of Easter and further in view of U.S. Patent No. 5,199,073 to Scott (hereinafter "Scott"). Applicant respectfully submits that claims 5 and 17 are not obvious over Yoshida in view of Easter and Scott.

With respect to claim 5, claim 5 depends from claim 2, and Applicant respectfully submits that Scott is not cited as curing, and does not cure, the deficiencies of Yoshida and Easter as discussed above with respect to claim 2. For at least these reasons, Applicant respectfully submits that claim 5 is allowable over Yoshida in view of Easter and Scott.

With respect to claim 17, claim 17 depends from claim 16, and Applicant respectfully submits that Easter and Scott are not cited as curing, and do not cure, the deficiencies of Yoshida as discussed above with respect to claim 16. For at least these reasons, Applicant respectfully submits that claim 17 is allowable over Yoshida in view of Easter and Scott.

Applicant respectfully requests that the §103 rejections be withdrawn.

New Claims

New claims 35 and 36 are added. Support for new claims 35 and 36 can be found in the specification at, for example, page 13, line 14 through page 14, line 6.

With respect to new claim 35, new claim 35 depends from claim 1 and Applicant respectfully submits that new claim 35 is allowable over the cited references at least because of its dependency on claim 1. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest the system of claim 1, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in new claim 35.

With respect to new claim 36, new claim 36 depends from claim 2 and Applicant respectfully submits that new claim 36 is allowable over the cited references at least because of its dependency on claim 2. Furthermore, Applicant respectfully submits that the cited references do not disclose or suggest the installation module of claim 2, wherein the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm as recited in new claim 36.

For at least these reasons, Applicant respectfully submits that new claims 35 and 36 are allowable over the cited references.

Conclusion

Claims 1-24, 26, 31-33, and 35-36 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned

attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 3/29/04

By: _____

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256